Aufgabe 1: Für eine Primzahl p bezeichne G_p die Menge aller Paare $(\overline{x}, \overline{y})$ in $\mathbb{F}_p \times \mathbb{F}_p$, sodass $\overline{x}^2 + 7\overline{y}^2 = 1$ gilt. Schreiben Sie mittels SAGE eine Funktion `order_of_Gp( p)`, die die Anzahl der Elemente von G_p zurückgibt. Berechnen Sie G_p für mindestens einhundert p und stellen Sie eine allgemeine Formel für die Anzahl der Element von G_p auf (sie müssen die Formel nicht beweisen, sie muss allerdings für alle von Ihnen berechneten Beispiele richtig sein).

```
def myFormula(p):
    if p== 7: return 14
    if p== 2: return 2
    else: # Fall 1: 7 ist kein Quadrat mod p:
          #   die Anzahl ist p +1 oder -1, je nachdem,
          #   ob p kongruent -1 mod 4 oder 1 mod 4 ist.
          # Fall 2: 7 ist ein Quadrat mod p:
          #   das Vorzeichen kehrt sich um

        if Mod(7,p).is_square(): vorzeichen= -1
        else: vorzeichen= 1

        if Mod(p,4) == 3: # p kongruent -1 mod 4
            return p - 1 * vorzeichen
        elif Mod(p,4) == 1:
            return p + 1 * vorzeichen

def order_of_p(p):
    G_p= GF(p)
    Lsgs= [(x,y) for x in G_p for y in G_p if x^2+7*y^2 == 1]

    return len(Lsgs)

p= 2 # firstPrime
Orders= {}
while len(Orders) < 100:
    # print p, (len(Orders))
    Orders[p] = order_of_p(p)
    if Orders[p] != myFormula(p):
        print "Falsch für",  p, " Wert:",Orders[p], \
          "mein Wert:", myFormula(p) , Mod(7,p).is_square()
        break
    #else:
    #    print "Richtig für", p, " Wert:",Orders[p], \
    #      "mein Wert:", myFormula(p), Mod(7,p).is_square()
    p = next_prime(p)
```

Aufgabe 2: Es bezeichnen X, Y und Z die Matrizen, die bei der natürlichen Operation von $\mathrm{GL}(3,\mathbb{R})$ auf $\mathbb{R}^3$ Drehungen um die x-, bzw. y- bzw. z-Achse entsprechen. Bestimmen Sie diese drei Matrizen. Berechnen Sie mittels SAGE die Untergruppe G von $\mathrm{GL}(3,\mathbb{Q})$, die von diesen drei Matrizen erzeugt wird (siehe `MatrixGroup()` in SAGE). Berechnen Sie (mittels SAGE) die Ordnung von G und für jeden Teiler d der Ordnung von G eine Liste der Elemente der Ordnung d. Zu welcher Ihnen schon bekannten Gruppe ist G wohl isomorph ...

Die Matrizen sind (siehe auch die allererste Übung):

$$X = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{bmatrix}, Y = \begin{bmatrix} \cos\alpha & 0 & -\sin\alpha \\ 0 & 1 & 0 \\ \sin\alpha & 0 & \cos\alpha \end{bmatrix}, Z = \begin{bmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

SAGE listet leider nicht die Elemente einer endlichen Matrixgruppe in Charakteristik 0. Andererseits sind alle Matrizen in G ja (offenbar) orthogonal und ganzzahlig[1]. Also erfüllt jede Zeile a, b, c von G die Identität $a^2 + b^2 + c^2 = 1$, insbesondere ist $|a|, |b|, |c| \leq 1$. Es genügt also über GF(3) zu rechnen:

```
sage: X = matrix( GF(3), 3, [1,0,0,0,0,-1,0,1,0])
sage: Y = matrix( GF(3), 3, [0,0,-1,0,1,0,1,0,0])
sage: Z = matrix( GF(3), 3, [0,-1,0,1,0,0,0,0,1])
sage: G = MatrixGroup( [X,Y,Z])
24
sage: od ={}
sage: for d in divisors(G.order()):
....:     od[d]= [g for g in G if g.order() == d]
....: od
```

Vermutung G und S_4 sind isomorph. Wir vergleichen die Elemente und Ordnungen in S_4:

```
sage: S4= SymmetricGroup(4)
sage: ods= {}
sage: for d in divisors(S4.order()):
....:     ods[d]= [g for g in S4 if g.order() == d]
....:
sage: for o in ods:
....:     print o,":", len(ods[o])
```

[1] Sinus und Kosinus nehmen nur die rationalen Werte $0, \pm\frac{1}{2}$ und ± 1 an. Für denselben Winkel α kommen nur die rationalen Wert 0 und ± 1 als Werte in Frage: es ist zwar $\sin(1/6\pi) = 1/2$ rational, dann ist aber $\cos(1/6 * \pi) = \sqrt{3}/2$ irrational und umgekehrt.

Und schließlich bestätigen wir unsere Vermutung:

```
sage: H=G.as_permutation_group()
sage: H.is_isomorphic(S4)
True
```

Aufgabe 3: Berechnen Sie mittels SAGE alle nichttrivialen Homomorphismen $\mathrm{SL}(2, \mathbb{F}_3) \to \mathbb{Z}/3\mathbb{Z}$. Hinweis: Ihre Freunde hierbei sind `IntegerModRing()`, `GF()`, `SL()` und `MatrixGroup()`.

Angenommen f ist ein Homomorphismus der angegebenen Art. Dann ist f surjektiv (denn jede Untergruppe von $\mathbb{Z}/3\mathbb{Z}$ ist trivial), und daher ist $\ker(f)$ eine normale Untergruppe vom Index 3 (d.h. der Ordnung 8) in $\mathbb{Z}/3\mathbb{Z}$ (nach dem ersten Isomorphiesatz).

Eine Untergruppe der Ordnung 8 muss Elemente der Ordnung 4 besitzen. Da in G nur die Ordnungen 1, 2, 3, 4, 6 vorkommen und es nur ein Element der Ordnung 2 in G gibt:

```
sage: G = SL(2,GF(3))
sage: len([g for g in G if g.order()==6])
8
sage: len([g for g in G if g.order()==3])
8
sage: len([g for g in G if g.order()==4])
6
sage: len([g for g in G if g.order()==2])
1
sage: len([g for g in G if g.order()==1])
1
sage: len([g for g in G if g.order()==8])
0
```

Wir bestimmen die Liste der Elemente der Ordnung 4:

```
sage: for x in G:
....:     if 4 == x.order():
....:         l.append(x)
sage: print len(l)
6
```

Und versuchen nun eine Untergruppe der Ordnung 8 aus ihnen zu konstruieren:

```
sage: a=l[0];b=l[2]
sage: H = MatrixGroup([a,b])
sage: H.order()
8
```

Nun prüfen wir, ob H bereits alle Elemente der Ordnung 4 enthält:

```
sage: len([h for h in H if h.order() == 4])
6
```

Wir haben eine Untergruppe der Ordnung 8 mit allen Elementen der Ordnung 4 bestimmt. Das ist der gesuchte Kernel von f. Es kann keine andere Teilmenge von G der Kernel sein, da der Kernel die Ordnung 8 hat und keine weiteren Elemente in G zur Verfügung stehen, ihre Ordnungen müsste ja 8 teilen. In $G \setminus H$ sind nur noch Elemente mit Ordnung 3 oder 6.

Wir suchen nun Elemente in G aber nicht in H:

```
sage: a,b = G.gens()
sage: a in H, a^2 in H
(False, False)
```

Damit sind a, a^2 Vertreter der nichtrivialen Nebenklassen in G=H, und wir können damit leicht die die beiden durch $a \mapsto 1$ bzw. $a \mapsto -1$ bestimmten Homomorphismen berechnen:

```
sage: B = IntegerModRing(3)
sage: f1 = dict()
sage: f2 = dict()
sage: for x in G:
....:     if x in H:
....:         f1[x] = B(0)
....:         f2[x] = B(0)
....:     elif a^-1 * x in H:
....:         f1[x] = B(1)
....:         f2[x] = B(-1)
....:     else:
....:         f1[x] = B(-1)
....:         f2[x] = B(1)
sage: f1
sage: f2
```

Aufgabe 4: Beweisen Sie die folgenden Aussagen:

1. Zu jeder natürlichen Zahl $N > 0$ gibt es genau eine Untergruppe der Ordnung N in $\mathbb{Q}/\mathbb{Z}$.

   Für alle $x \in G := \mathbb{Q}/\mathbb{Z}$ gilt $Nx \in \mathbb{Z}$, da $0+\mathbb{Z} = \mathbb{Z}$ das neutrale Element in G ist und jedes Element von G stets N oder einen Teiler von N als Ordnung hat.

   Es gilt also $Nx \in \mathbb{Z} \Leftrightarrow x \in \left\{q \in \mathbb{Q} \,\middle|\, q = \frac{k}{N}, k \in \mathbb{Z}\right\} = \langle \frac{1}{N} \rangle$.

   Fazit: alle $x \in G$ sind von der Form $\frac{k}{N}+\mathbb{Z}$, das ist genau die Untergruppe $\left\{\frac{1}{N} + \mathbb{Z}, \frac{2}{N} + \mathbb{Z}, \ldots, \frac{N}{N} + \mathbb{Z} = 0 + \mathbb{Z}\right\}$ von $\mathbb{Q}/\mathbb{Z}$.

2. Die Gruppe $\mathbb{Q}/\mathbb{Z}$ ist isomorph zur Untergruppe μ_∞ aller Elemente endlicher Ordnung in $\mathbb{S}^1$. Hinweis: Zeigen Sie, dass $t \mapsto \cos(2\pi t) + i \sin(2\pi t)$ einen Gruppenhomomorphismus $\mathbb{R} \to \mathbb{S}^1$ definiert, und wenden Sie in geeigneter Art und Weise den ersten Isomorphiesatz an.

   Wir betrachten die Menge

   $$K := \{(x, y) \,|\, x = \cos(2\pi t), y = \sin(2\pi t), t \in \mathbb{R}\}\,.$$

   Aus der Analysis ist bekannt, dass K der Einheitskreis ist. Indem wir Realteil und Imaginärteil mit x und y Koordinate identifizieren, können wir K und $S^1 = \{z \in \mathbb{C} \,|\, z = \cos(2\pi t) + i \sin(2\pi t), t \in \mathbb{R}\}$ miteinander identifizieren. (S^1 ist der Einheitskreis in der komplexen Ebene.)

   Wir müssen zeigen, dass die Abbildung $\phi : \mathbb{R} \to S^1$ einen Gruppenhomomorphismus darstellt. Dazu zeigen wir $\phi(a + b) = \phi(a)\phi(b)$, mittels der Additionstheoreme[2] von Sinus und Kosinus.

   $$\begin{aligned}
   \phi(a+b) &= \cos(2\pi(a+b)) + i\sin(2\pi(a+b)) \\
   &= \big(\cos(2\pi a)\cos(2\pi b) - \sin(2\pi a)\sin(2\pi b)\big) + \\
   &\quad i\big(\sin(2\pi a)\cos(2\pi b) + \cos(2\pi a)\sin(2\pi b)\big) \\
   \phi(a)\cdot\phi(b) &= \big(\cos(2\pi a) + i\sin(2\pi a)\big)\cdot\big(\cos(2\pi b) + i\sin(2\pi b)\big) \\
   &= \big(\cos(2\pi a)\cos(2\pi b) - \sin(2\pi a)\sin(2\pi b)\big) + \\
   &\quad i\big(\cos(2\pi a)\sin(2\pi b) + \sin(2\pi a)\cos(2\pi b)\big)
   \end{aligned}$$

   Die Abbildung ist ein Homomorphismus.

[2] In der Funktionentheorie lernt man $\exp(2\pi i t) = \cos(2\pi t) + i \sin(2\pi t)$. Mit der Funktionalgleichung der (komplexen) Exponentialfunktion folgt die Behauptung dann sofort.

Die Abbildung $g : \mathbb{Q} \to S^1$, die einen Bruch $\frac{k}{n}$ auf $g(\frac{k}{n}) = \cos(2\pi\frac{k}{n}) + i\sin(2\pi\frac{k}{n})$ abbildet, hat den Kern $\mathbb{Z}$, wegen der Periodizität der Winkelfunktionen.

Wie in Teil 1 sieht man, dass jedes Element endlicher Ordnung n von S^1 bereits zu einem Winkel $2\pi\frac{k}{n}$ gehört, wobei $k = 1, \ldots, n$ gilt.

Deswegen ist die Abbildung g surjektiv. Nach dem ersten Isomorphiesatz ist die Abbildung g eine Isomorphie von $\mathbb{Q}/\mathbb{Z}$ nach μ_∞.